CENTER FOR DIGITAL DEMOCRACY

The Center for Digital Democracy (CDD) endorses the Federal Trade Commission's (FTC) proposal to better protect health consumer and patient information in the digital era. CDD warned the commission in 2010, as well as in its 2022 commercial surveillance comments, that health data—including information regarding serious medical conditions—are routinely (and cynically) gathered and used for online marketing. This has placed Americans at risk—for loss of their privacy, health-decision autonomy, and personal financial security. The commercial surveillance health data digital marketing system also triggers major strains on the fiscal well-being of federal and private health insurance systems, creating demand for products and services that can be unnecessary and costly.

The commission should "turn off the tap" of data flooding the commercial surveillance marketplace, including both direct and inferred health information. The commission can systemically address the multiple data flows—including those on Electronic Health Record (EHR) systems—that require a series of controls. EHR, or personal health record systems, have served as a digital "Achilles heel" of patient privacy, with numerous commercial entities seizing that system to influence physicians and other prescribers as well as to gain insights used for ongoing tracking. The commercialization of health-connected data is ubiquitous, harvested from mobile "apps," online accounts, loyalty programs, social media posts, data brokers, marketing clouds and elsewhere. Given the contemporary commercial data analytic affordances to generate insights and actions operational today, information gathered for other purposes can be used to generate health-related data. Health information can be combined with numerous other datasets that can reveal ethnicity, location, media use, etc., to create a robust target marketing profile. As programmatic advertising trade publication "AdExchanger" recently noted, "sensitive health data can be collected or revealed through dozens of noncovered entities, from location data providers to retail media companies. And these companies aren't prevented from sharing data, unless the data was sourced from a covered entity."

The FTC's Health Breach Notification Rule (HBNR) proposal comes at an especially crucial time for health privacy in the U.S. A recent report on "The State of Patient Privacy," as noted by Insider Intelligence/eMarketer in July 2023, shows that a majority of Americans "distrust" the role that "Big Tech Companies" play with their health data. A majority of patients surveyed explained that "they are worried about security and privacy protections offered by vendors that handle their health data." Ninety-five percent of the patients in the survey "expressed concern about the possibility of data breaches affecting their medical records." These concerns, we suggest, reflect consumer unease regarding their reliance on the online media to obtain health information. For example, "half of US consumers use at least one health monitoring tool," and "healthcare journeys often start online," according to the "Digital Healthcare Consumer 2023"

report. There is also a generational shift in the U.S. underway, where at least half of young adults (so-called Generation Z) now "turn to social media platforms for health-related purposes either all the time or often…via searches, hashtags QR codes…[and] have the highest rate of mobile health app usage." The Covid-19 pandemic triggered greater use of health-related apps by consumers. So-called "telehealth" services generate additional data as well, including for online "lead generation." The growing use of "digital pharmacies" is being attributed to the rising costs of medications—another point where consumer health data is gathered.

The FTC should ensure the health data privacy of Americans who may be especially vulnerable—such as those confronting financial constraints, pre-existing or at-risk conditions, or have long been subjected to predatory and discriminatory marketing practices—and who are especially in need of stronger protections. These should include addressing the health-data-related operations from the growing phalanx of retail, grocery, "dollar," and drug store chains that are expanding their commercial surveillance marketing operations (so-called "retail media"), while providing direct-to-consumer delivered health services.

Electronic Health Record systems are a key part of the health and commercial surveillance infrastructure: EHRs have long served as "prime real estate for marketers…[via] data collection, which makes advanced targeting a built-in benefit of EHR marketing." EHRs are used to influence doctors and other prescribers relying on what's euphemistically called point-of-care marketing. Marketing services for pharmaceutical and other life science companies can be "contextually integrated into the EHR workflow [delivered] to the right provider at the right time within their EHR [using] awareness messaging targeted on de-identified real-time data specific to the patient encounter." Such applications are claimed to operate as "ONC-certified and HIPPA-compliant (ONC stands for "Office of the National Coordinator for Health Information," HHS). The various, largely unaccountable, methods used to target and influence how physicians treat their patients by utilizing EHRs raise numerous privacy and consumer protection issues. For example, "EHR ads can appear in several places at all the stages along the point-of-care journey," one company explained. Through an "E-Prescribing Screen," pharma companies are able to offer "co-pay coupons, patient savings offers and relevant condition brand messaging."

Data used to target physicians, including prescription information derived from a consumer, using EHR systems, help trigger more information from and about a health consumer (think about the subsequent role of drug stores, search engines and social media use, gathering of data for coupons, etc.). This "non-virtuous" circle of health surveillance should be subjected to meaningful health data breach and security safeguards. Patient records on EHRs must be safeguarded and the methods used to influence healthcare professionals require major privacy reforms.

Contemporary health data systems reflect the structures that comprise the overall commercial surveillance apparatus, including databrokers, marketing clouds, AI: The use of digital marketing to target U.S. health consumers has long been a key "vertical" for advertisers. For example, there are numerous health-focused subsidiaries run by the leading global advertising agencies, all of which have extensive data-gathering and targeting capabilities. These include Publicis Health: "Our proprietary data and analytics community, paired with the unsurpassed strengths of Sapient and Epsilon allow us to deliver unmatched deterministic,

behavioral, and transactional data, powered by AI." IPG Health uses "a proprietary…media, tech and data engine [to] deliver personalized omnichannel experiences across touchpoints." Its "comprehensive data stack [is] powered by Acxiom." Ogilvy Health recently identified some of the key social media strategies used by pharmaceutical firms to generate consumer engagement with their brands—helping generate invaluable data. They include, for example, a "mobile-first creative and design approach," including the use of "stickers, reels, filters, and subtitles" on Instagram and well as "A/B testing" on Facebook and the use of "influencers." A broad range of consumer-data-collecting partners also operates in this market, providing information and marketing facilitation. Google, Meta, Salesforce, IQVIA, and Adobe are just a few of the companies integrated into health marketing services designed to "activate customer journeys (healthcare professionals and patients) across physical and digital channels [using] real-time, unified data." Machine learning and AI are increasingly embedded in the health data surveillance market, helping to "transform sales and marketing outcomes," for example. The use of social media, AI and machine learning, including for personalization, raises concerns that consent is insufficient alone for the release of patient and consumer health information. The commission should adopt its proposed rule, but also address the system-wide affordances of commercial surveillance to ensure health data is truly protected in terms of privacy and security.

The commission should endorse a patient health record information definition that reflects both the range and type of data collected, but also the processes used to gather or generate it. The prompting and inducement of physicians, for example, to prescribe specific medications or treatments to a patient, based on the real-time "point-of-care" information transmitted through EHRs, ultimately generate identifiable information. So any interaction and iterative process used to do so should be covered under the rule, reflecting all the elements involved in that decision-making and treatment determinative process. By ensuring that all the entities involved in this system—including health care services or suppliers—must comply with data privacy and security rules, the commission will critically advance data protection in the health marketplace. This should include health apps, which increasingly play a key role in the commercial data-driven marketing complex. All partnering organizations involved in the sharing, delivering, creating and facilitation of health record information should also be held accountable.

We applaud the FTC's work in the health data privacy area, including its important GoodRx case and its highlighting the role that "dark patterns" play in "manipulating or deceiving consumers." Far too much of the U.S. health data landscape operates as such a "dark pattern." The commission's proposed HBNR rules will illuminate this sector, and, in the process, help secure greater privacy and protection for Americans.